Claims 1-40 are now pending.

As described in the application, a system and method are provided for use in distributing access to a data item (e.g., book data). For example, at a publisher computer, publisher permission data is stored that allows a number A of end-user computers to gain access to an encrypted book data item. Based on the publisher permission data, a distributor computer is provided with distributor permission data that allows a number B of end-user computers to gain access to the encrypted book data item. The publisher permission data is changed so that the publisher permission data allows only a number A-B of end-user computers to gain access to the encrypted book data item. Based on the distributor permission data, a retailer computer is provided with retailer permission data that allows a number C of end-user computers to gain access to the encrypted book data item. The distribution permission data is changed so that the distributor permission data allows only a number B-C of end-user computers to gain access to the encrypted book data item. Based on the retailer permission data, an end-user computer is provided with end-user permission data that allows 1 end-user computer to gain access to the encrypted book data item, wherein the end-user permission data may be used to gain access to a piece of the encrypted book data item at a time. The retailer permission data is changed so that the retailer permission data allows only a number C-1 of end-user computers to gain access to the encrypted book data item.

All of the independent claims (1, 20-40) have been amended. All of the independent claims make clear that that the encrypted data or data item has paged subsets or pages that are accessible a paged subset or page at a time using the same instance of permission for each paged subset or page. Support may be found in the specification at least at page 15, lines 10-12, and at least in the specification's descriptions of book oriented data items (books being well known for having paged subsets known as pages).

All of the claims have been rejected over U.S. Patent No. 5,109,413 to Comerford et al ("Comerford") in view of U.S. Patent No. 5,629,980 to Stefik et al ("Stefik"), or over Comerford in view of Stefik and further in view of U.S. Patent No. 6,230,267 to Richards et al ("Richards").

Comerford discloses a software asset protection mechanism that segregates the right to execute software from the software itself. The rights to execute, when installed on a composite computing system, are stored in a coprocessor element of the composite computing system. The

software asset protection mechanism is provides for the manipulation of those rights to execute. The rights to execute can be conditioned in terms of a valid period of execution or a valid number of executions. The rights to execute can be safely transferred from one coprocessor to another, or can be returned to the software vendor. A method of backing up the rights to execute provides the user with the rights to execute in the event the coprocessor element of the composite computing system fails.

Stefik discloses a system for controlling use and distribution of digital works. The owner of a digital work attaches usage rights to that work. Usage rights are granted by the "owner" of a digital work to "buyers" of the digital work. The usage rights define how a digital work may be used and further distributed by the buyer. Each right has associated with it certain optional specifications which outline the conditions and fees upon which the right may be exercised. Digital works are stored in a repository. A repository will process each request to access a digital work by examining the corresponding usage rights. Digital work playback devices, coupled to the repository containing the work, are used to play, display or print the work. Access to digital works for the purposes of transporting between repositories (e.g. copying, borrowing or transfer) is carried out using a digital work transport protocol. Access to digital works for the purposes of replay by a digital work playback device (e.g. printing, displaying or executing) is carried out using a digital work playback protocol.

Richards discloses a method and apparatus for securely transporting data onto an IC card. The method is used, for example, to transport data, including application programs, in a secure manner from a source located outside the IC card. At least a portion of the data is encrypted using the public key of a public/secret key pair of the intended IC card unit. The encrypted data is then sent to the IC card and the IC card verifies the key transformation unit using its unique secret key. The data can then be stored on the IC card. A copy of the public key signed by a certification authority can be used to verify that the card is authorized to be part of the overall authorized system.

The action states that the method disclosed in Comerford differs from the claimed invention since the right to execute in Comerford permits a user to access software. The applicant submits that Comerford is in even further removed from the claimed invention in that Comerford is directed to giving the user the right to execute software.

In addition, the claims, which are directed to distributing access to a data item, have been amended to make clear that the encrypted data or data item has paged subsets or pages that are accessible a paged subset or page at a time using the same instance of permission for each paged subset or page. Comerford teaches nothing about gaining access to a paged subset or page of encrypted data at a time. The action states that Stefik teaches allowing access to a piece of encrypted data at a time at col. 3, lines 13-29:

> U.S. Pat. No. 5,247,575, Sprague et al., entitled "Information Distribution System", describes an information distribution system which provides and charges only for user selected information. A plurality of encrypted information packages (IPs) are provided at the user site, via high and/or low density storage media and/or by broadcast transmission. Some of the IPs may be of no interest to the user. The IPs of interest are selected by the user and are decrypted and stored locally. The IPs may be printed, displayed or even copied to other storage medias. The charges for the selected IP's are accumulated within a user apparatus and periodically reported by telephone to a central accounting facility. The central accounting facility also issues keys to decrypt the IPs. The keys are changed periodically. If the central accounting facility has not issued a new key for a particular user station, the station is unable to retrieve information from the system when the key is changed.

However, the cited teaching merely discloses that multiple encrypted information packages may be provided at a user site. By contrast, the claims specifically require not only that the encrypted data or data item have paged subsets or pages that are accessible a paged subset or page at a time but also that the same instance of permission is used for each paged subset or page. As previously recognized, Comerford does not even suggest as much. With respect to the specific rejections, the cited Comerford-based combinations lack any disclosure whatsoever regarding paged subsets or pages that are accessible a paged subset or page at a time using the same instance of permission for each paged subset or page as required by the claims.

The dependent claims are patentable for at least the same reasons stated above in connection with the independent claims.

The applicant submits that the application is in condition for allowance, which action is requested.

The Commissioner is hereby authorized to charge the extra claim fee, if any, to our Deposit Account No. 08-0219. The Commissioner is also authorized to charge any other fee required to maintain the pendency of the application, or to credit any overpayment to Deposit Account No. 08-0219.

Respectfully submitted,

Dated: November 14, 2002

Jason A. Reyes
Registration No. 41,513
Attorney for Applicants

Hale and Dorr LLP
60 State Street
Boston, MA 02109
Tel.: (617) 526-6010
Fax: (617) 526-5000

Replacement Pages for Claims 1-40

(MARKED TO SHOW CHANGES)

1. A method for use in distributing access to a data item, comprising:

allowing multiple transfers between computers of a single instance of permission to gain access to an encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same instance of permission for each paged subset, the transfers occurring across data connections and including a first transfer between a first computer and a second computer and a subsequent transfer between the second computer and a third computer, wherein at any one time only one computer retains the instance of permission and is able to use the instance of permission to gain access to a paged subset [piece] of the encrypted data item at a time.

2. The method of claim 1, further comprising:

using an encryption key to impede unauthorized access to the encrypted data item.

3. The method of claim 1, wherein at least one of the transfers of permission includes the transfer of a first encryption key.

4. The method of claim 3, further comprising:

using a second encryption key to encrypt the first encryption key prior to transfer.

5. The method of claim 4, wherein the first encryption key includes a secret key and the second encryption key includes one of the keys in a public/private key set.

6. The method of claim 1, further comprising:

using highly secure circuitry to help ensure that at any one time only one of the computers retains and is able to use the instance.

7. The method of claim 6, wherein the highly secure circuitry includes a smartcard computer.

8. The method of claim 6, wherein the highly secure circuitry includes a de-encryptor.

9. The method of claim 6, further comprising:

storing an encryption key in the highly secure circuitry.

10. The method of claim 9, further comprising:

using the encryption key only within the highly secure circuitry.

11. The method of claim 1, further comprising:

determining whether a computer is authorized to receive the instance of permission to gain access to the encrypted data item.

12. The method of claim 1, further comprising:

according to an expiration time, rendering at least one of transfers temporary.

13. The method of claim 12, further comprising:

in the temporary transfer, transmitting a copy of an encryption key from a sender computer to a recipient computer, and, at the expiration time, erasing the copy of the encryption key from the recipient computer.

14. The method of claim 1, further comprising:

in one of the transfers, transmitting a copy of an encryption key from a sender computer to a recipient computer, and erasing the copy of the encryption key from the sender computer.

15. The method of claim 1, further comprising:

associating at least one of the transfers with a transfer of funds.

16. The method of claim 1, further comprising:

distinguishing between different instances of permission to gain access to the encrypted data item.

17. The method of claim 1, wherein at least one of the computers includes a Web server computer.

18. The method of claim 1, wherein at least one of the computers includes a book viewing device.

19. The method of claim 18, wherein the book viewing device includes a viewing screen and data communications circuitry.

20. A method comprising:

in accordance with access distribution parameters that are specific to an encrypted data item and that were established by a first computer, transferring, across a data connection from a second computer to a third computer and independently of the first computer, permission to gain access to the encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the

permission may be used to gain access to a paged subset [piece] of the encrypted data item at a time.

21. A method comprising:

impeding a change to the number of computers that are allowed to gain access to an encrypted data item, independently of data connection transfers between computers of permission to gain access to the encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset [piece] of the encrypted data item at a time.

22. A method for use in distributing access to a data item, comprising:

providing a first computer with permission to gain access to an encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset [piece] of the encrypted data item at a time;

providing the permission by data connection to a second computer and removing the permission from the first computer; and

providing the permission by data connection to a third computer and removing the permission from the second computer.

23. A method comprising:

rendering accountably fungible an instance of permission data that allows a computer to gain access to encrypted book data, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same instance of permission for each paged subset, wherein the instance of permission data may be used to gain access to a paged subset [piece] of the encrypted book data at a time.

24. A method for use in distributing access to a book data item, comprising:

associating highly secure circuitry with a device that is able to send and receive access data that is necessary to gain access to an encrypted book data item, the encrypted book data item having paged subsets that are accessible a paged subset at a time using the same access data for each paged subset, wherein the access data may be used to gain access to a paged subset [piece] of the encrypted book data item at a time, the highly secure circuitry including a computer

processor and a program memory and being able to help an unauthorized transfer of the access data from the device.

25. A method for use in distributing access to a book data item, comprising:

at a publisher computer, storing publisher permission data that allows a number A of end-user computers to gain access to an encrypted book data item;

based on the publisher permission data, providing a distributor computer with distributor permission data that allows a number B of end-user computers to gain access to the encrypted book data item;

changing the publisher permission data so that the publisher permission data allows only a number A-B of end-user computers to gain access to the encrypted book data item;

based on the distributor permission data, providing a retailer computer with retailer permission data that allows a number C of end-user computers to gain access to the encrypted book data item;

changing the distribution permission data so that the distributor permission data allows only a number B-C of end-user computers to gain access to the encrypted book data item;

based on the retailer permission data, providing an end-user computer with end-user permission data that allows 1 end-user computer to gain access to the encrypted book data item, the encrypted book data item having paged subsets that are accessible a paged subset at a time using the same end-user permission data for each paged subset, wherein the end-user permission data may be used to gain access to a paged subset [piece] of the encrypted book data item at a time; and

changing the retailer permission data so that the retailer permission data allows only a number C-1 of end-user computers to gain access to the encrypted book data item;

wherein number A-B is non-negative, number B-C is non-negative, and number C-1 is non-negative.

26. A system for use in distributing access to a data item, comprising:

data processing apparatus for allowing multiple transfers between computers of a single instance of permission to gain access to an encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same instance of permission for each paged subset, the transfers occurring across data connections and including a first transfer between a first computer and a second computer and a subsequent transfer between the

second computer and a third computer, wherein at any one time only one computer retains the instance of permission and is able to use the instance of permission to gain access to the encrypted data item, wherein the instance of permission may be used to gain access to a paged subset [piece] of the encrypted data item at a time.

27. A system comprising:

a transferor, in accordance with access distribution parameters that are specific to an encrypted data item and that were established by a first computer, transferring, across a data connection from a second computer to a third computer and independently of the first computer, permission to gain access to the encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset [piece] of the encrypted data item at a time.

28. A system comprising:

an impedor impeding a change to the number of computers that are allowed to gain access to an encrypted data item, independently of data connection transfers between computers of permission to gain access to the encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset [piece] of the encrypted data item at a time.

29. A system for use in distributing access to a data item, comprising:

a first permission provider providing a first computer with permission to gain access to an encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset [piece] of the encrypted data item at a time;

a second permission provider providing the permission by data connection to a second computer and removing the permission from the first computer; and

a third permission provider providing the permission by data connection to a third computer and removing the permission from the second computer.

30. A system comprising:

a renderor rendering accountably fungible an instance of permission data that allows a computer to gain access to encrypted book data, the encrypted book data having paged subsets

that are accessible a paged subset at a time using the same instance of permission data for each paged subset, wherein the instance of permission data may be used to gain access to a paged subset [piece] of the encrypted book data at a time.

31. A system for use in distributing access to a book data item, comprising:

a device including highly secure circuitry, the device being able to send and receive access data that is necessary to gain access to an encrypted book data item, the encrypted book data having paged subsets that are accessible a paged subset at a time using the same access data for each paged subset, wherein the access data may be used to gain access to a paged subset [piece] of the encrypted book data item at a time, the highly secure circuitry including a computer processor and a program memory and being able to help prevent an unauthorized transfer of the access data from the device.

32. A system for use in distributing access to a book data item, comprising:

at a publisher computer, a storer for storing publisher permission data that allows a number A of end-user computers to gain access to an encrypted book data item;

a first permission provider for, based on the publisher permission data, providing a distributor computer with distributor permission data that allows a number B of end-user computers to gain access to the encrypted book data item;

a first permission changer for changing the publisher permission data so that the publisher permission data allows only a number A-B of end-user computers to gain access to the encrypted book data item;

a second permission provider for, based on the distributor permission data, providing a retailer computer with retailer permission data that allows a number C of end-user computers to gain access to the encrypted book data item;

a second changer for changing the distribution permission data so that the distributor permission data allows only a number B-C of end-user computers to gain access to the encrypted book data item;

a third permission provider for, based on the retailer permission data, providing an end-user computer with end-user permission data that allows 1 end-user computer to gain access to the encrypted book data item, the encrypted book data item having paged subsets that are accessible a paged subset at a time using the same end-user permission data for each paged

subset, wherein the end-user permission data may be used to gain access to a paged subset [piece] of the encrypted book data item at a time; and

a third changer for changing the retailer permission data so that the retailer permission data allows only a number C-1 of end-user computers to gain access to the encrypted book data item;

wherein number A-B is non-negative, number B-C is non-negative, and number C-1 is non-negative.

33. Computer software, residing on a computer-readable medium, comprising instructions for use in distributing access to a data item, the instructions causing a computer to:

allow multiple transfers between computers of a single instance of permission to gain access to an encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same instance of permission for each paged subset, the transfers occurring across data connections and including a first transfer between a first computer and a second computer and a subsequent transfer between the second computer and a third computer, wherein at any one time only one computer retains the instance of permission and is able to use the instance of permission to gain access to the encrypted data item, wherein the instance of permission may be used to gain access to a paged subset [piece] of the encrypted data item at a time.

34. Computer software, residing on a computer-readable medium, comprising instructions for causing a computer to:

in accordance with access distribution parameters that are specific to an encrypted data item and that were established by a first computer, transfer, across a data connection from a second computer to a third computer and independently of the first computer, permission to gain access to the encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset [piece] of the encrypted data item at a time.

35. Computer software, residing on a computer-readable medium, comprising instructions for causing a computer to:

impede a change to the number of computers that are allowed to gain access to an encrypted data item, independently of data connection transfers between computers of

permission to gain access to the encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset [piece] of the encrypted data item at a time.

36. Computer software, residing on a computer-readable medium, comprising instructions for use in distributing access to a data item, the instructions causing a computer to:

provide a first computer with permission to gain access to an encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset [piece] of the encrypted data item at a time;

provide the permission by data connection to a second computer and removing the permission from the first computer;

provide the permission by data connection to a third computer and removing the permission from the second computer.

37. Computer software, residing on a computer-readable medium, comprising instructions for causing a computer to:

render accountably fungible an instance of permission data that allows a computer to gain access to encrypted book data, the encrypted book data having paged subsets that are accessible a paged subset at a time using the same instance of permission data for each paged subset, wherein the instance of permission data may be used to gain access to a paged subset [piece] of the encrypted book data at a time.

38. Computer software, residing on a computer-readable medium, comprising instructions for use in distributing access to a book data item, the instructions causing a computer to:

associate highly secure circuitry with a device that is able to send and receive access data that is necessary to gain access to an encrypted book data item, the encrypted book data item having paged subsets that are accessible a paged subset at a time using the same access data for each paged subset, wherein the access data may be used to gain access to a paged subset [piece] of the encrypted book data item at a time, the highly secure circuitry including a computer processor and a program memory and being able to help an unauthorized transfer of the access data from the device.

39. Computer software, residing on a computer-readable medium, comprising instructions for use in distributing access to a book data item, the instructions causing a computer to:

at a publisher computer, store publisher permission data that allows a number A of end-user computers to gain access to an encrypted book data item;

based on the publisher permission data, provide a distributor computer with distributor permission data that allows a number B of end-user computers to gain access to the encrypted book data item;

change the publisher permission data so that the publisher permission data allows only a number A-B of end-user computers to gain access to the encrypted book data item;

based on the distributor permission data, provide a retailer computer with retailer permission data that allows a number C of end-user computers to gain access to the encrypted book data item;

change the distribution permission data so that the distributor permission data allows only a number B-C of end-user computers to gain access to the encrypted book data item;

based on the retailer permission data, provide an end-user computer with end-user permission data that allows 1 end-user computer to gain access to the encrypted book data item, the encrypted book data item having paged subsets that are accessible a paged subset at a time using the same end-user permission data for each paged subset, wherein the end-user permission data may be used to gain access to a paged subset [piece] of the encrypted book data item at a time; and

change the retailer permission data so that the retailer permission data allows only a number C-1 of end-user computers to gain access to the encrypted book data item;

wherein number A-B is non-negative, number B-C is non-negative, and number C-1 is non-negative.

40. A method for use in distributing access to a data item, comprising:

allowing multiple transfers between computers of a single instance of permission to gain access to an encrypted book data item, the encrypted book data item having pages that are accessible a page at a time using the same instance of permission for each page, the transfers occurring across data connections and including a first transfer between a first computer and a second computer and a subsequent transfer between the second computer and a third computer,

wherein at any one time only one computer retains the instance of permission and is able to use the instance of permission to gain access to a page of the encrypted book data item at a time for display purposes.